Payment Card Industry (PCI) Compliance
A QSA Perspective
Agenda

- Introduction
- Getting Started
- Data Flows
- Gap Assessment
- Remediation
What is Payment Card Industry (PCI)?

– Industry imposed mandate to secure cardholder data, enforced through contractual obligations and managed or supported by the following participating organizations:
  • Payment Brands (VISA, Mastercard, American Express, Discover and JCB)
  • Merchant or Acquiring Banks (VISA and Mastercard Member Banks)
  • Payment Card Industry Security Standards Council (PCI-SSC) “The PCI Council”
  • Qualified Security Assessors (QSAs)
  • Authorized Scan Vendors (ASVs)
  • Others
– Provides for a set of Security Standards (PCI-DSS, PA-DSS and PCI-PTS)
– Includes Payment Brand Compliance Programs (CISP, SDP, DSOP, DISC and DSP) which;
  • Define criteria for assignment of merchant and service provider levels
  • Set compliance dates for member financial institutions, merchants and service providers
  • Levy fines against member financial institutions, merchants and service providers in the event of non-compliance and/or data breach
  • Investigate all account data compromises and are responsible for associated forensic response
What Do PCI Terms Mean?

– Payment Brand – VISA, Mastercard, American Express, Discover and JCB.

– PCI-SSC – Independent industry standards body founded by the payment brands to provide oversight regarding the development and management of Payment Card Industry Security standards.

– Merchant – Organization accepting payment from cardholders.

– Service Provider – Business entity directly involved in the processing, storage, transmission, or switching of transaction data, or cardholder data on behalf of other merchants or service providers.

– Acquirers – Can be Payment Brands in the case of American Express and Discover or member banks that initiate and maintain relationships with merchants accepting payment cards as part of VISA and Mastercard bankcard associations.

– Issuer – Issue the credit card to the cardholder and each time the cardholder makes a purchase, provides transaction authorization to the merchant’s acquiring bank.

– PCI-DSS – Standard consisting of 12 sections containing 250 plus controls. This document is used by Qualified Security Assessors (QSAs) to conduct an on-site assessment and prepare a Report on Compliance (RoC). The RoC is used by Level 1 Merchants to validate/report compliance to Acquiring banks or Payment Brands.
What Do PCI Terms Mean?

– Self-Assessment Questionnaire – A high-level questionnaire used by Merchants Level 2 and below to demonstrate/report compliance to Acquiring banks or Payment Brands.

– Qualified Security Assessor (QSA) – Qualified Security Assessor (QSA) companies are organizations that have been qualified by the PCI Council. Qualified Security Assessors are employees of these organizations who have been certified by the PCI Council to validate an entity’s adherence to the PCI-DSS.

– Approved Scanning Vendors (ASVs) – Organizations that have been qualified by the PCI Council to perform vulnerability scans of merchants’/service providers’ Internet-facing environments.

– Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorization during transactions when the card is presented.

– Sensitive Authentication Data – This term is used to describe the Card Validation Code or Value (CVV, CVC, and CSC) section of Full Track and the Card-Not-Present (CNP) Value (CVV2, CVC2, and CID).

– Tokenization – The substitution of a primary account number (PAN) with a token (e.g., a serial number) from which the original PAN can not be independently derived. If stolen, tokens are of no monetary value.
What are Merchant Levels?

There appears to be significant confusion regarding how merchant levels are determined and how they affect the way in which a merchant becomes compliant.

- Merchant levels (e.g., 1 through 4) allow payment brands to stratify the risk of their merchant populations and apply specific validation and reporting requirements to them.

- Merchant levels are determined by transaction volume per card type on an annual basis (e.g., VISA considers any merchant conducting over 6 million VISA transactions per year to be a level 1).

- Beyond transaction volume criteria, payment brands and acquiring banks reserve the right to assign merchant levels arbitrarily. My advice to merchants, always verify your level with your payment brand or acquiring bank.

- Merchant level does not affect compliance requirements, it affects validation and reporting requirements. All merchants, regardless of level, must be in compliance with the entire PCI-DSS, but depending on their level, they may validate and report compliance to their payment brand or acquiring bank differently.

- Each payment brand has published criteria for determining merchant levels along with associated validation and reporting requirements on their respective compliance program (CISP, SDP, DSOP, DISC and DSP) websites. Realize these criteria may vary.
Who Needs to Comply and Why?

– The Who
  • Merchants
  • Service Providers
  • Acquiring Banks
  • Issuers
  • Any entity that stores, processes, or transmits cardholder data.

– The Why
  • Payment Brands and Acquiring Banks include PCI-DSS compliance provisions in all contracts with their member financial institutions, their service providers and their merchants.
  • Failure to demonstrate compliance in a timely manner can result in substantial fines which are detailed in each payment brand’s compliance program.
  • Data Breach Costs can be substantial including:
    ➢ Forensics and Legal
    ➢ Consumer Notification and Card Replacement
    ➢ Brand Damage
    ➢ Fines (compliance related and egregious violations)
How to Get Started?

– Include PCI in your audit universe. This can be a high-level inquiry to determine if your organization stores, transmits or processes cardholder data. It can be even more high-level; does your organization have any contracts in place which include obligations to become PCI compliant?

– If it is determined your organization has PCI compliance obligations, work to secure additional resources to support a detailed analysis including a cardholder data flow and PCI gap assessment. A more detailed analysis will provide the necessary context regarding PCI risks facing the organization.

– Use the resulting audit report generated from the cardholder data flow and PCI gap assessment to present the case to executive leadership. PCI programs are resource intensive, they have organizational impact and can’t be managed effectively by information technology organizations alone, executive support is essential.

– Once it is established a PCI program needs to exist, someone has to own it. We all too often see PCI program ownership relegated to project managers with little ability to marshal the necessary resources (e.g., establish budgets, influence indirect reports, etc). Our experience indicates PCI program ownership should be someone in the CIO’s organization, Director level equivalent or above. The PCI program owner should be a direct report of executive leadership.
Foundational Compliance Tasks

Gap Assessment

Data Flow Diagrams

In-Scope System Listing

Cardholder Data Matrix
Data Flow Overview

- The Data Flow exercise is one of the most important prerequisites in determining where an organization stands regarding compliance, as well as defining the road map to becoming PCI compliant.

- The Data Flow is just one of the many PCI-DSS requirements, so many organizations don’t understand the importance of completing a Data Flow or just don’t know this task is foundational to a successful PCI program.

- Start by defining the Data Flow Methodology you will follow throughout the exercise, the most common methodology is interview based.

- Understand Data Flow tasks should create multiple outputs (e.g., Data Flow Diagrams, In-Scope System Listing and Cardholder Data Matrix) and that each is crucial to managing a PCI program.

- Understand the difference between a Process Flow and a Data Flow. Most auditors use process flows on a regular basis, but the concept of a data flow might be foreign.

- Allocate adequate time to conduct the Data Flow exercise. A general rule of thumb is 8 to 10 hours per process. Also, understand during this effort previously unknown cardholder systems may be uncovered and additional time might need to be allocated.
Data Flow Methodology

– It’s common to start with a large meeting including all personnel that have a role within PCI, where a high-level sketch of the flow of cardholder data can be revealed.

– This initial meeting will help identify all the entry and exit points for cardholder data within the environment and all stops/routes/storage along the way.

– Identify the process owners for each system involved with the flow of cardholder data, this will determine the initial interviews.

– Setup interviews with all the cardholder data entry point process owners and follow the data as it flows through the environment. The line of questioning should be simple, such as “where does data go next” or “and then what”. The flow of data should be followed until it ends, including any paper processes.

– There are several key data points which must be collected in order to understand where all cardholder data is stored, processed and transmitted. You should collect system information (e.g., O/S type, version and server name), database platform (e.g., type, version, database names and table names), application name (e.g., type and version), network equipment types (e.g., platform and version) and connectivity details (e.g., VPN, MPLS, POTS, wireless, private line, etc). You should also understand what data is stored and how. Is more than the PAN stored; is the PAN encrypted; and how long is the PAN stored? Don’t forget paper processes!
Process Flow vs. Data Flow

- Many people tend to confuse or combine the terms Process Flow and Data Flow. Within the context of PCI, it is important to “understand the process” and “flow the data.”
# Cardholder Data Matrix Example

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>FILE/TABLE TYPE</th>
<th>DESC</th>
<th>FILE/TABLE NAME</th>
<th>RETENTION</th>
<th>CC No.</th>
<th>Name</th>
<th>Exp Date</th>
<th>Track Pin</th>
<th>Directory Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCCPXXXYY*</td>
<td>Log File</td>
<td>Transnet NFM Log</td>
<td>Log.txt</td>
<td>1 Day</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\SAP\transnet\logs</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>CAB File</td>
<td>Transnet Log Backup</td>
<td>eftlog####ymmdss.cab</td>
<td>8 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\logbkup1</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>CAB File</td>
<td>Transnet Log Backup</td>
<td>eftlog####ymmdss.cab</td>
<td>8 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\logbkup2</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>CAB File</td>
<td>Transnet Log Backup</td>
<td>eftlog####ymmdss.cab</td>
<td>8 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\logbkup3</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>CAB File</td>
<td>Transnet Log Backup</td>
<td>eftlog####ymmdss.cab</td>
<td>8 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\logbkup4</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>CAB File</td>
<td>Transnet Log Backup</td>
<td>eftlog####ymmdss.cab</td>
<td>8 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\logbkup5</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>CAB File</td>
<td>Transnet Log Backup</td>
<td>eftlog####ymmdss.cab</td>
<td>8 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\logbkup6</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>CAB File</td>
<td>Transnet Log Backup</td>
<td>eftlog####ymmdss.cab</td>
<td>8 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\logbkup7</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>CAB File</td>
<td>Transnet Log Backup</td>
<td>eftlog####ymmdss.cab</td>
<td>8 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\logbkup8</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>Binary</td>
<td>Real Time Xpress Server Transaction Log</td>
<td>ssssr####.txn</td>
<td>14 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\retail systems\Xpress Server</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>Binary</td>
<td>Real Time POS Transaction Log</td>
<td>LD.txt</td>
<td>7 Days</td>
<td>E</td>
<td>E</td>
<td>Y</td>
<td>N</td>
<td>c:\sap\retail systems\Point of Sale\RDATA</td>
</tr>
<tr>
<td>SSCCPXXXYY*</td>
<td>Text File</td>
<td>XPS Log</td>
<td>clogyyyyymmd.txt</td>
<td>3 Days</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td>N</td>
<td>c:\sap\retail systems\Xpress Server\SDATA</td>
</tr>
</tbody>
</table>
## In-Scope System Listing Example

<table>
<thead>
<tr>
<th>Appl</th>
<th>PCI</th>
<th>Loc #</th>
<th>Prefix</th>
<th>System Name</th>
<th>IP Address</th>
<th>Description</th>
<th>OS</th>
<th>Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS</td>
<td>Encr</td>
<td>33</td>
<td>RST</td>
<td>RST033-1</td>
<td>10.34.3.233</td>
<td>POS Restaurant Application/DB Server</td>
<td>W2K3</td>
<td>Dbase</td>
</tr>
<tr>
<td>POS</td>
<td>Encr</td>
<td>34</td>
<td>RST</td>
<td>RST034-1</td>
<td>10.34.3.233</td>
<td>POS Restaurant Application/DB Server</td>
<td>W2K3</td>
<td>Dbase</td>
</tr>
<tr>
<td>POS</td>
<td>Encr</td>
<td>37</td>
<td>RST</td>
<td>RST037-1</td>
<td>10.34.3.233</td>
<td>POS Restaurant Application/DB Server</td>
<td>W2K3</td>
<td>Dbase</td>
</tr>
<tr>
<td>POS</td>
<td>Encr</td>
<td>38</td>
<td>RST</td>
<td>RST038-1</td>
<td>10.34.3.233</td>
<td>POS Restaurant Application/DB Server</td>
<td>W2K3</td>
<td>Dbase</td>
</tr>
<tr>
<td>POS</td>
<td>Encr</td>
<td>63</td>
<td>RST</td>
<td>RST063-1</td>
<td>10.34.3.233</td>
<td>POS Restaurant Application/DB Server</td>
<td>W2K3</td>
<td>Dbase</td>
</tr>
<tr>
<td>POS</td>
<td>Encr</td>
<td>64</td>
<td>RST</td>
<td>RST064-1</td>
<td>10.34.3.233</td>
<td>POS Restaurant Application/DB Server</td>
<td>W2K3</td>
<td>Dbase</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>63</td>
<td>GB</td>
<td>GB63</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>64</td>
<td>GB</td>
<td>GB64</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>1</td>
<td>MN</td>
<td>MN001</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>2</td>
<td>MN</td>
<td>MN002</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>3</td>
<td>MN</td>
<td>MN003</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>4</td>
<td>MN</td>
<td>MN004</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>5</td>
<td>MN</td>
<td>MN005</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>6</td>
<td>MN</td>
<td>MN006</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>7</td>
<td>MN</td>
<td>MN007</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>8</td>
<td>MN</td>
<td>MN008</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>9</td>
<td>MN</td>
<td>MN009</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
<tr>
<td>POS</td>
<td>Hash</td>
<td>10</td>
<td>MN</td>
<td>MN010</td>
<td>10.34.3.233</td>
<td>POS Database Server</td>
<td>AIX</td>
<td>Informix</td>
</tr>
</tbody>
</table>
Gap Assessment Overview

– Begin by developing an overall understanding of the cardholder data environment to be assessed. This step is often skipped, but can be accomplished through review of cardholder data flows, a cardholder data matrix and an in-scope system listing prior to initiating a PCI gap assessment.

– Define the scope of the PCI gap assessment following your documentation review. This step will likely require network architecture analysis and interaction with various system owners.

– Define your sampling methodology, each unique cardholder system component and environment must be represented.

– Use the PCI-DSS which includes detailed testing procedures, not the SAQ.

– Conduct testing based on PCI-DSS stated testing procedures, don’t omit or modify any of the test steps, doing so may result in testing outcomes which would be inconsistent with outcomes produced by QSAs.

– Prepare work papers and collect/retain evidence just as you would for any other audit. A meaningful assessment cannot be conducted with interviews alone.

– Realize gap assessments are “Tip of the Spear” efforts and that it’s better from a remediation perspective to have compliant areas listed as non-compliant initially rather than the other way around.
How to Scope The Gap Assessment

- You must have a complete understanding of the number of applications, databases and systems that store, process, or transmit cardholder data.

- You must have a complete understanding of the physical locations that have systems that store, process or transmit cardholder data.

- You should have completed a cardholder data matrix which documents systems storing cardholder data, the data stored, specific storage location (e.g., database table name or file name), reason for storage, retention period and protection mechanism employed.

- You should have performed a cardholder data discovery (e.g., scanning and network traffic monitoring) to confirm the information contained within the cardholder data matrix is accurate and complete.

- You must understand which system components (e.g., firewalls, routers and switches, wireless devices, etc) make up the various environments’ perimeters and you must verify effective network segmentation is in place if you intend to exclude non-cardholder systems from the scope of the assessment.

- You must understand under what circumstances a system can be excluded from the assessment’s scope.
Limit Scope with Segmentation

“Without adequate network segmentation (sometimes called a “flat network”) the entire network is in scope of the PCI-DSS assessment”.

Segmentation must include strong access control lists with the following characteristics and considerations:

- Limit access to only the ports or services required.
- Limit access by user or if necessary IP address to only those with a justified/documentated business need.
- Do not allow “Risky” protocols such as FTP or Telnet.
- Consider Two-factor authentication or Network Access Control for the segmented network.
“Flat Network” Discussion

No Segmentation

All workstations and wireless networks are in scope for all PCI DSS requirements.

All servers are in scope for all PCI DSS requirements.

All external facing systems are in scope for all PCI DSS requirements.

All systems storing or processing CHD are in scope for all PCI DSS requirements.
Segmented Network Discussion

*With Segmentation*

- All workstations that access CHD are in scope for all PCI DSS requirements.
- If no CHD is used on wireless network then it is out of scope.
- All external facing systems are in scope for all PCI DSS requirements.
- All systems storing or processing CHD are in scope for all PCI DSS requirements.
Limit Scope with Data Elimination

– The fastest way to reduce the scope of a PCI gap assessment is to eliminate the storage, processing and transmission of cardholder data on as many systems as possible.

– The following methods can be used to reduce PCI scope with some limitations:
  • Remove the PAN.
  • Truncate the PAN, leaving only the first 6 and last 4 digits.
  • One-Way Hash the PAN.
  • Tokenize the PAN.

– The following limitations apply to the methods above:
  • Although a system may not store the PAN, it may still process or transmit it and is therefore still in-scope.
  • Systems that receive PAN before it’s truncated, hashed or tokenized or that do the actual truncation, hashing or tokenization are still in-scope.
  • Systems that don’t store transmit or process cardholder data, but are directly connected to the cardholder environment are still in-scope.

– Remember, encrypted cardholder data is still cardholder data and any system storing, processing and transmitting it is still in-scope.
Gap Assessment Sampling Guidance

– Sampling is completely acceptable when performing testing, but the method(s) used must represent the populations of business facilities and systems components. The PCI Council does not dictate specific sampling methods (e.g., statistical sampling), but they want the sampling rationale and method(s) documented.

– When selecting sample sizes, take into consideration the uniqueness of the environments from a process, network architecture and system component perspective.

  • Standard processes, system components and network architectures in place with centralized management across all business facilities? Then a smaller sample is sufficient to provide reasonable assurance. A general rule of thumb would be typically 3-5 for each homogenous population of facilities and system components (specific situations may warrant different sampling).

  • No standard processes, system components or network architectures in place with decentralized management across business facilities? Then a larger sample is required to provide reasonable assurance. A general rule of thumb would be up to 10% of the population up to 25 maximum (specific situations may warrant different sampling).

– When selecting samples understand they should be rotated from year to year.

– Refer to PCI-DSS Appendix F for more information regarding the process for selecting samples.
PCI-DSS Versus SAQ

Why use the PCI-DSS instead of the SAQ? Because the testing outcomes can be vastly different when testing procedures are omitted.

<table>
<thead>
<tr>
<th>SAQ</th>
<th>PCI-DSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Are vendor-supplied defaults always changed before installing a system on the network? Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</td>
<td>2.1 Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</td>
</tr>
<tr>
<td>2.1 Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor supplied accounts and passwords.)</td>
<td></td>
</tr>
</tbody>
</table>
Don’t Skip or Alter Test Procedures

– Even when using the PCI-DSS the tendency is to short-cut testing. Why should I try and log on when I can just review the configuration files, etc? Because, in some cases the default configuration might not be displayed in the configuration file. The best way to validate vendor supplied defaults have been changed is to actually attempt to use them to access the system.

PCI-DSS

| 2.1 Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts. |
| 2.1 Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor supplied accounts and passwords.) |
Completing the Gap Assessment

– As mentioned previously, we consider gap assessments a “Tip of the Spear” effort. In other words, gap assessments are the initial entry point mechanism allowing management to understand whether PCI controls need their attention and whether additional investigation is necessary.

– It is all too common to see gap assessments stalled and incomplete because the sheer volume of controls and testing are overwhelming. This is why gap assessment efforts must be treated as an initial entry point, they must be used to identify deficiencies in the relevant populations, but once identified, deficiencies should be noted and the effort should move on to completion. “Don’t let the perfect be the enemy of the good”.

– The identification of deficiencies in a control area should almost always result in follow-on investigation during remediation efforts which we’ll discuss shortly. This “break in contact” between the gap assessment and the follow-on investigation allows for the timely completion of the gap assessment while still providing a mechanism for comprehensive understanding.

– When a control’s compliance status is in doubt, designate it as non-compliant so it can be considered during follow-on investigation activities. This will ensure all questionable controls are considered once the necessary subject matter expertise is assembled.
Remediation Strategies Overview

- It is assumed at this point the building blocks discussed in the previous slides are in place. These include completed cardholder data flows, cardholder data matrix, in-scope system listing and gap assessment documents.

- The building blocks are leveraged to construct an overall remediation strategy. This includes organizing each identified non-compliant control into remediation classes (e.g., Application Development, Documentation, Encryption, Network Security, Physical Security, Platform Security and Authentication Data). Remediation class groupings are then leveraged to aggregate high-level tasks based on operational/technical synergies into various remediation projects.

- Project charters are established for each of the areas outlined in the Project Strategy document. Project charters should contain overall project description, which specific controls are included and it should define project team members.

- Once established, project teams consisting of necessary subject matter expertise should work with the group that performed the gap assessment to understand the nature of the deficiencies and perform more detailed testing and analysis to validate initial findings and establish the actual scope of necessary remediation.

- Following complete validation and definition of deficiencies, remediation efforts can begin with detailed solution set design.
## Remediation Strategy Example

### Remote Access

<table>
<thead>
<tr>
<th>Scope</th>
<th>The scope of this project includes investigating two-factor authentication options/vendors, testing selection and deploying selection to all remote users connecting through IPSEC and/or SSL VPN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS Sections</td>
<td>Tasks / Requirements</td>
</tr>
<tr>
<td>8.3</td>
<td>Implement two-factor authentication for all users with remote access to the cardholder environment.</td>
</tr>
<tr>
<td>1.3.9, 5.1</td>
<td>Implement or verify personal firewalls and anti-virus for all systems connecting to the cardholder environment remotely.</td>
</tr>
<tr>
<td>Dependencies</td>
<td>N/A</td>
</tr>
<tr>
<td>Groups Involved</td>
<td>Network Security, Network Services, Operations</td>
</tr>
<tr>
<td>Effort</td>
<td>High</td>
</tr>
<tr>
<td>Timeline</td>
<td>6 Months</td>
</tr>
</tbody>
</table>

### Non-Console Administration

<table>
<thead>
<tr>
<th>Scope</th>
<th>The scope of this project includes investigating alternate non-console administration technologies (SSH, VPN, SSL/TLS), selecting technology and implementing technology to all in scope systems, including UNIX, wireless access points, and routers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS Sections</td>
<td>Tasks / Requirements</td>
</tr>
<tr>
<td>2.3</td>
<td>Require the use of encrypted non-console administration technologies (SSH, SSL, etc) and discontinue the use of clear text protocols (e.g., Telnet) when connecting to UNIX, wireless access points, and routers.</td>
</tr>
<tr>
<td>8.4 a</td>
<td>Encrypt password transmissions for UNIX and routers. Configuration of encrypted non-console administration technologies will satisfy this requirement.</td>
</tr>
<tr>
<td>Dependencies</td>
<td>N/A</td>
</tr>
<tr>
<td>Groups Involved</td>
<td>Network Security, Network Services, Operations</td>
</tr>
<tr>
<td>Effort</td>
<td>Low</td>
</tr>
<tr>
<td>Timeline</td>
<td>2 Months</td>
</tr>
</tbody>
</table>
Remediation Strategy Example

Example PCI Compliance Program Timeline

LEGEND
- Authentication Data
- Encryption
- Network Security
- Documentation
- Application Development
- Platform Security
- Physical Security

© 2010 Protiviti Inc. An Equal Opportunity Employer. CONFIDENTIAL: This document is for your company’s internal use only and may not be copied nor distributed to another third party.
Questions?

Dan Reyero, Managing Director

protiviti

5005 LBJ Freeway
Suite 1100
Direct: 469.374.2547
Mobile: 817.291.7441
Fax: 972.788.8563
Dan.Reyero@protiviti.com

Powerful Insights. Proven Delivery.™

Brad McGary, Senior Manager, QSA

protiviti

5005 LBJ Freeway
Suite 1100
Direct: 469.374.2533
Mobile: 972.740.4597
Fax: 469.374.2615
Brad.McGary@protiviti.com

Powerful Insights. Proven Delivery.™

Jacob Iley, Senior Manager, QSA

protiviti

5005 LBJ Freeway
Suite 1100
Direct: 469.374.2486
Mobile: 214.906.7380
Fax: 469.374.2690
Jacob.Iley@protiviti.com

Powerful Insights. Proven Delivery.™
Powerful Insights. Proven Delivery.